

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent of:	) Confirmation No.: 3198
Stefan Andersson	)
Application No.: 09/977,192	) Examiner: Jeffrey L. Williams
Filing Date: October 16, 2001	) Art Unit: 2137
For: SECURITY SYSTEM	)

**PETITION PURSUANT TO 37 CFR §1.181 TO RECOGNIZE JUNE 20, 2007, AS THE ACTUAL START OF TIME PERIOD UNDER 37 CFR 41.37(d) AND AS DEFINED IN MPEP § 1205.03 WITHIN WHICH TO FILE AN AMENDED BRIEF, AND TO REFUND THE FEE PAID FOR A FIVE-MONTH EXTENSION OF TIME UNDER 37 CFR 1.136**

**MAIL STOP PETITION**

**ATTN: DIRECTOR OF TECHNOLOGY CENTER 2100**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

The Commissioner is hereby petitioned:

- to recognize June 20, 2007, as the actual mailing date of the Notification of Non-Compliant Appeal Brief (37 CFR 41.37) dated December 26, 2006 (hereinafter referred to as “the Notification” and attached hereto as Exhibit A);
- to recognize that Applicant’s Response to Notification of Non-Compliant Appeal Brief (hereinafter referred to as “the Response” and attached hereto as Exhibit B) filed on June 25, 2007, timely complied with 37 CFR 41.37(d) in that it was filed well within the longer of one month or 30 days of the actual mailing date of the Notification; and
- in view of the foregoing, to refund to the undersigned the extension of time fee paid, via an online credit card transaction (RAM), along with the Response.

The grounds for this petition are as follows:

1. The undersigned represents the above-identified Applicant before the U.S. Patent

and Trademark Office (USPTO).

2. On June 20, 2007, Examiner Jeffrey L. Williams telephoned the undersigned to inquire whether a response to the Notification had been filed. It was at that time that the undersigned first became aware of the Notification.

3. Immediately after terminating the call with Examiner Williams, the undersigned downloaded a copy of the Notification from the USPTO PAIR website. According to the downloaded copy, the Notification had supposedly been mailed on December 26, 2006 (the day after the Christmas holiday), and had a one-month response due date of January 26, 2007.

4. On June 25, 2007, five days after first becoming aware of the Notification, the undersigned prepared and filed the Response and a Petition for a Five-Month Extension of Time (hereinafter “the Petition” and attached hereto as Exhibit C) along with the fee of \$2160.00 to ensure that the Response would be considered by the Office, and to avoid any possibility of abandonment in light of June 26, 2007 technically being the latest possible date that a response could be filed with extensions of time.

5. Around the time of filing the Response and Petition, the undersigned conducted an investigation of his firm’s records to uncover any evidence of receipt of the Notification. Attached hereto as Exhibit D is a copy of a docket report (redacted to ensure the confidentiality of information about unrelated applications) showing which responses were coming due on January 26, 2007 (i.e., the date corresponding to the one-month response due date of the Notification). Also attached as Exhibit E is a copy of a mail log (redacted to ensure the confidentiality of information about unrelated applications) showing entries of USPTO related mail received by the firm between December 11, 2006 and February 8, 2007, which is a time period the undersigned’s firm would have reasonably expected to receive any mail addressed to the firm and deposited with the U.S. Post Office on December 26, 2006. Attachments D and E do not include any indication that the undersigned’s firm received and/or docketed the Notification.

6. Because the undersigned had no knowledge of the Notification until receiving the courtesy call from the Examiner on June 20, 2007, the first time the undersigned was “given

or mailed” the Notification actually occurred on June 20, 2007. Consequently, the undersigned should have been given “one month or 30 days” starting from June 20, 2007, thus making the undersigned’s Response of June 25, 2007 timely without requiring the Petition for a Five-Month Extension of Time and the accompanying \$2160.00 fee.

7. While the undersigned believed payment of the extension of time fee should not have been required for consideration of the Response, he was left with no realistic alternative course of action that would have ensured that the application would not become abandoned. Thus, in response to the Examiner’s call of June 20, 2007, the undersigned took the initiative of downloading the Notification and promptly responding to the requirements of the Notification to ensure that the appeal would not become dismissed and the application subsequently abandoned as of January 26, 2007 (See, MPEP 1215.04). If the undersigned had done nothing on or before June 26, 2007, or had submitted a response without an extension of time fee, the USPTO would likely have issued a Notice of Abandonment, which in turn would have resulted in the undersigned filing a Petition to Withdraw Holding of Abandonment, getting that Petition granted, and responding to a “new” copy of the Notification with a “new” response period. However, such alternative courses of actions do not advance the proceedings in a meaningful or efficient way or appear to act in the best interests of the Applicant.

8. Accordingly, the undersigned respectfully requests relief pursuant to the Commissioner’s authority under 37 CFR §1.181 in the form of recognizing June 20, 2007, as the effective mailing date of the Notification and refunding the \$2160.00 extension of time fee paid by the undersigned via an online credit card transaction (RAM).

Respectfully submitted,  
Potomac Patent Group PLLC

Date: October 15, 2007

By: /Kenneth B. Leffler, Reg. No. 36,075/  
Kenneth B. Leffler  
Registration No. 36, 075

P.O. Box 270  
Fredericksburg, Virginia 22404  
703-718-8884

## **EXHIBIT A**



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,192	10/16/2001	Stefan Andersson	027557-071	3198
42015	7590	12/26/2006	EXAMINER	
POTOMAC PATENT GROUP, PLLC P. O. BOX 270 FREDERICKSBURG, VA 22404			ART UNIT	PAPER NUMBER

DATE MAILED: 12/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Notification of Non-Compliant Appeal Brief (37 CFR 41.37)</b>	<b>Application No.</b> 09/977,192	<b>Applicant(s)</b> ANDERSSON, STEFAN	
	<b>Examiner</b> Jeffery Williams	<b>Art Unit</b> 2137	

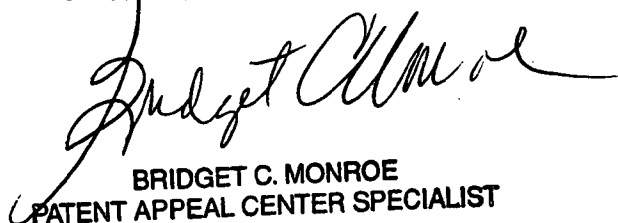
--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on 24 November 2006 is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer.  
**EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.
2. ☐ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).
3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).
4. ☐ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).
5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi)).
6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).
7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).
8. ☒ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and **relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).
9. ☒ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).
10. ☒ Other (including any explanation in support of the above items):

The brief is missing headings Evidence Appendix and Related Proceedings Appendix, if there are none an indication of "None" or "Not Applicable" is required.

  
BRIDGET C. MONROE  
PATENT APPEAL CENTER SPECIALIST

## **EXHIBIT B**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	<b>MAIL STOP Appeal Brief – Patents</b>
	)	
Stefan ANDERSSON	)	Group Art Unit: 2137
	)	
Application No.: 09/977,192	)	Examiner: WILLIAMS, Jeffery L.
	)	
Filed: October 16, 2001	)	Confirmation No.: 3198
	)	
For: SECURITY SYSTEM	)	

**RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is a response to the Notification of Non-Compliant Appeal Brief purportedly mailed by the Office on December 26, 2007. A Petition for Five-Month Extension of Time and corresponding required fee are concurrently herewith. However, Applicant intends to file a request for refund of the fee because the Notification of Non-Compliant Appeal Brief was never received by Applicant. Applicant first became aware of the Notification of Non-Compliant Appeal Brief as a result of a courtesy call made on June 20, 2007 (i.e., already into the fifth-month extension period) by Examiner Williams inquiring whether a Response to the Notice had already been filed. This response is prepared based on a copy of the Notification that was obtained from Private PAIR on June 20, 2007.

Applicant's Remarks begin on page 2 of this paper.

An Amended Appeal Brief is being filed concurrently herewith.



## REMARKS

The Notification of Non-Compliant Appeal Brief alleges that the Appeal Brief filed on November 24, 2006 is Non-Compliant because of two defects described as follows:

“8. The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and relied upon by appellant in the appeal, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. Other (including any explanation in support of the above items):

The brief is missing headings Evidence Appendix and Related Proceedings Appendix, if there are none an indication “None” or “Not Applicable” is required”

Applicant respectfully traverses the allegation that the Appeal Brief filed on November 24, 2006 is non-compliant. 37 CFR 41.37(c)(1)(ix) states, in relevant part, “An appendix containing copies of any evidence submitted pursuant to §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the examiner and relied upon by appellant in the appeal, along with a statement setting forth where in the record that evidence was entered in the record by the examiner. ...” Applicant is not relying on any such evidence, and therefore has no copies to include in the appendix. Nothing in the regulation indicates that that an empty section must be included in the Brief if there are no “copies” to include. Even if one turns to the M.P.E.P for guidance on the Office’s internal policy concerning this issue, at most M.P.E.P. §1205.02, page 1200-15 (Rev. 3, August 2005) states “If there is no evidence being relied upon by appellant in the appeal, then an evidence appendix should be included with the indication ‘none.’” (Emphasis added.) It is well known that the word “should” is permissive, and does not require that a thing be done or included. (Compare with the word “must”, which indicates that something is mandatory.) Thus, the Appeal Brief is

not *per se* non-compliant for failing to include an Evidence Appendix when there is no evidence to submit.

Similarly, 37 CFR 41.37(c)(1)(x), in its totality, states “An appendix containing copies of decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of this section.” In this instance, there are no court or Board proceedings identified pursuant to paragraph (c)(1)(ii) of 37 CFR 41.37. Therefore, Applicant has no copies to include in this appendix. Nothing in the regulation indicates that that an empty section must be included in the Brief. Even if one turns to the M.P.E.P. for guidance on the Office’s internal policy concerning this issue, at most M.P.E.P. §1205.02, page 1200-15 (Rev. 3, August 2005) states “If there are no such copies of decisions being submitted in the appeal, then a related proceedings appendix should be included with the indication ‘none.’” (Emphasis added.) Since the word “should” is permissive (i.e., it does not require that a thing be done or included), the Appeal Brief is not *per se* non-compliant for failing to include a Related Proceedings Appendix when there are no related proceedings documents to submit.

Regardless of whether the Office agrees with Applicant’s interpretation of the word “should”, attention is directed to M.P.E.P. §1205.03, pages 1200-16 through 1200-17 (“Non-compliant Appeal Brief and Amended Brief”) which states:

The examiner should not require a corrected brief for minor non-compliance in an appeal brief (e.g., the brief has a minor error in the title of a section heading). The following are a few other examples where the examiner may accept a brief that has minor non-compliance:

(A) If the evidence appendix and related proceedings appendix are missing, but the record is clear that there is no evidence submitted and no related proceedings listed in the related appeals and interferences section, the examiner may accept the brief and state in the examiner’s answer that it is assumed that the appellant meant to include both appendixes with a statement of “NONE.”

(Emphasis added.)

Thus, in the present instance, the Examiner should have accepted the already-filed brief without requiring any “correction.”

Notwithstanding the above arguments, in order to expedite favorable prosecution of the application, filed concurrently herewith is an amended copy of the Appeal Brief with new appendix sections IX and X added to show where copies of evidence and court decisions would have been placed had there been any.

In view of the above, it is respectfully requested that the amended Appeal Brief be accepted, and the Appeal be allowed to continue. If the Office has any remaining questions or concerns about the Appeal Brief, it is requested that a call be placed to the undersigned attorney at 703.718.8884 to expedite resolution of any such issues.

Respectfully submitted,

Potomac Patent Group PLLC

Date: June 25, 2007

P.O. Box 270  
Fredericksburg, Virginia 22404  
703-718-8884

By: /Kenneth B. Leffler, Reg. No. 36,075/  
Kenneth B. Leffler  
Registration No. 36,075

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of	)	<b>MAIL STOP Appeal Brief – Patents</b>
	)	
Stefan ANDERSSON	)	Group Art Unit: 2137
	)	
Application No.: 09/977,192	)	Examiner: WILLIAMS, Jeffery L.
	)	
Filed: October 16, 2001	)	Confirmation No.: 3198
	)	
For: SECURITY SYSTEM	)	

**APPEAL BRIEF**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal was filed on July 26, 2006. In support of that Appeal, this Appeal Brief is being filed concurrently with the required fee specified by 37 C.F.R. §41.20(b)(2). As the due date for this Appeal Brief is determined to be one month from the mailing date of the Notice of Panel Decision from Pre-Appeal Brief Review (i.e., one month from October 3, 2006), this Appeal Brief in conjunction with the Petition for One-Month Extension of Time plus applicable petition fees (filed concurrently herewith) is believed to be timely filed.

Favorable reconsideration and reversal of the various rejections are respectfully requested in view of the following remarks.

**I. REAL PARTY IN INTEREST**

The real party in interest in connection with this application is Telefonaktiebolaget L M Ericsson, by virtue of an Assignment executed by the inventor (Stefan ANDERSSON) on January 7, 2002, and recorded in the U.S. Patent and Trademark Office at Reel 012476, Frame 0738.

**II. RELATED APPEALS AND INTERFERENCES**

Applicant is unaware of any related appeals or interferences in connection with this application.

**III. STATUS OF CLAIMS**

Claims 20-23 and 31 have been canceled. The remaining claims 1-19, 24-30, and 32-50 stand rejected. The rejection of claims 1-19, 24-30, and 32-50 is appealed.

**IV. STATUS OF AMENDMENTS**

Applicant filed an After-Final Amendment on July 25, 2006 with proposals to amend a number of paragraphs of the specification. An Advisory Action mailed on August 4, 2006 informs that the proposed amendments will not be entered because they allegedly raise the issue of new matter.

**V. SUMMARY OF CLAIMED SUBJECT MATTER**

As explained in the application at page 1, line 11 through page 2, line 4, it is known to provide cryptographic functionality to support an application (e.g., e-mail or internet browser) which requires cryptography in a computer. As an example, U.S. Patent No. 5,689,565 describes a cryptography system architecture for a computer. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The system further includes at least one cryptographic service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys.

This system architecture is used in many applications in which data may desirably be transferred across unsecured computer networks such as the internet. For example, this architecture can be used in applications such as e-mail clients, web browsers, and the like. A

similar architecture can be used for access control within a computer system, and for hard disc encryption.

It is advantageous not to maintain cryptographic keys and/or algorithms on the same computer hardware as the application(s) because anyone with unauthorized access to the computer would have access to these as well. Solutions known at the time of Applicant's invention suffer from a drawback in that, in addition to the computer, the user is required to carry with him/her extra equipment, such as an IC card and/or an IC card reader capable of connecting to the computer. The IC card is used for storing the cryptographic keys used by the CSP in the computer.

Applicant's invention addresses this problem, thereby reducing the burden on users, by establishing a synergistic relationship between the computer and another device that the user would ordinarily be carrying regardless of any planned computer usage: a mobile station (e.g., a cellular telephone). As explained in the specification at page 4, line 29 through page 5, line 21, mobile stations typically include their own cryptographic module for enabling encrypted communication over a wireless interface with a network, such as through a Wireless Application Protocol (WAP) Gateway. Encryption in these cases provides confidentiality for users.

Thus, as explained in the specification at page 5, line 22-28, in accordance with embodiments of the invention, the cryptographic module of the phone, and other features which are used to provide secure communication using the Wireless Application Protocol, also allow the mobile station (e.g., phone 30) (see FIGS. 1, 4, and 5) to provide some or all of the functionality of a cryptography service provider to the computer. In this way, the need to carry extraneous equipment just to perform the computer's cryptographic functions is eliminated. Instead, the computer determines that it requires cryptographic services, and establishes a connection to the mobile station to obtain these services (e.g., FIG. 2, steps 100-108). The requested cryptographic operation is carried out (e.g., FIG. 2, step 110; and FIG. 3, step 136), and the result of the cryptographic operation is passed from the phone back to the computer (e.g., FIG. 3, step 138). The computer then ensures that the application requesting the cryptographic operation receives the result of that operation (e.g., FIG. 2, steps 112-114), and the computer carries on its own operations without the need to further involve the mobile station.

Various embodiments defined by the claims will now be described with reference to the specification and drawings. It should be understood that any such reference (e.g., to

specification text and/or elements/steps illustrated in the figures) is intended to be exemplary only. No inference should be made that the elements/steps being discussed are not also described and/or illustrated in other places of the application, possibly in connection with other embodiments.

Accordingly, embodiments defined by independent claim 1 are directed to:

1. A method of encrypting communications from a computer (e.g., the computers 10, 60) having an application program interface (e.g., CAPI 18), the method comprising:
  - initiating communications from said computer over a computer network (e.g., specification at page 3, lines 26-30);
  - determining that encryption of said communications is required (e.g., specification at page 3, line 31 through page 4, line 8);
  - establishing a connection with a mobile communications device (e.g., specification at page 6, lines number 1-4; FIG. 1: connection between CSP\*26 and MS 30; FIG. 2: step 104; FIG. 4: connection between CSP\*26 and MS 30; FIG. 5: connection between CT\* 76 and MS 30; and FIG. 6: step 164), wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network (e.g., specification at page 5, lines 12 -21; FIG. 1: SIM-WIM 32; FIG. 4: SIM-WIM 32; FIG. 5: SIM-WIM 32); and
  - using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer (e.g., specification at page 7, line 33 through page 8, line 3; FIG. 2: steps 108-110; page 11, through page 12, line 4; and FIG. 6: steps 166-168) over said computer network without sending said encrypted communications over said wireless communications network (e.g., specification at page 8, lines 4-7 and FIG. 2: steps 112-114; specification at page 12, lines 5-8; and FIG. 6: step 170).

Embodiments defined by independent claim 7 are directed to:

7. A mobile communications device, comprising:
  - means for communicating over a wireless interface with a wireless communications network (e.g., specification at page 4, lines 20-33);

means for connection to a remote computer without involving the wireless communications network (e.g., specification at page 3, lines 26-30); and  
a cryptographic module (e.g., SIM-WIM 32), the cryptographic module being usable:  
for encoding wireless communications from the device over said wireless interface (e.g., specification at page 5, lines 6-21);  
by a cryptographic service provider with an application program interface of the remote computer (e.g., specification at page 5, lines 22-28).

It is noted that the “means for communicating over a wireless interface” and the “means for connection to a remote computer” are defined in terms of means-plus-function as permitted by 35 U.S.C. § 112, sixth paragraph. Exemplary supporting structure/material/acts for these elements are described in the application as indicated above.

Embodiments defined by independent claim 19 are directed to:

19. A tangible module for a personal computer (e.g., CSP\* 26), wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network (e.g., FIG. 2, steps 100-102), the module sends a second command to a mobile communication device (e.g., FIG. 2, step 104), the mobile communication device having a cryptographic module (e.g., SIM-WIM 32) for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer (e.g., FIG. 2, step 110) allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 24 are directed to:

24. A system, comprising:  
a computer (e.g., PC 10); and



a mobile communications device (e.g., MS 30), including a cryptographic module (e.g., SIM-WIM 32) for performing cryptographic functions in mobile communication over a wireless communications network,

the computer having at least one application (e.g., e-mail application 14; browser 16) which requires cryptographic functionality for communication over a computer network,

a first part of the required cryptographic functionality being provided in the computer (e.g., SHA-1 algorithm functionality that can be provided on the CSP\* 26 – see specification at page 6, lines 24-26), and a second part of the required cryptographic functionality being provided in the mobile communications device (e.g., RSA algorithm functionality that can be provided on the MS 30 – see specification at page 6, lines 26-28),

the computer and the mobile communications device having means for establishing a secure communications path therebetween (e.g., specification at page 6, lines 1-16); and

the computer further comprising an interface device (e.g., CAPI 18) which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

It is noted that the “means for establishing a secure communications path therebetween” (i.e., between the computer and the mobile communications device) are defined in terms of means-plus-function as permitted by 35 U.S.C. §112, sixth paragraph. Exemplary supporting structure/material/acts for these elements are described in the application as indicated above.

Embodiments defined by independent claim 28 are directed to:

28. A method of encrypting communications from a computer having an application program interface (e.g., CAPI 18), wherein the communications are over a computer network (e.g., specification at page 3, lines 26-30), the method comprising:

sending data to be encrypted from the computer to a mobile communications device (e.g., FIG. 2, step 108), wherein the mobile communications device has a cryptographic module (e.g., SIM-WIM 32) for performing cryptographic functions in communications over a wireless communications network (e.g., specification at page 5, lines 6-21), and further, wherein the mobile communications device uses the cryptographic module to encrypt the data (e.g., specification at page 5, lines 22-28);

receiving encrypted data at the computer from the mobile communications device (e.g., FIG. 3, step 138); and

using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 36 are directed to:

36. A system for supporting an application (e.g., e-mail application 14; browser 16), the system comprising:

a computer (e.g., PC 10) including:

a cryptographic application program interface (e.g., CAPI 18); and

a cryptography service provider (e.g., CSP\* 26); and

a mobile communication device (e.g., MS 30) including a cryptographic module (e.g., SIM-WIM 32),

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface sends a command to the cryptography service provider (e.g., FIG. 2, steps 102-104), and

wherein the cryptography service provider has a communications link to the cryptographic module of the mobile communications device (e.g., specification at page 6, lines number 1-4; FIG. 1: connection between CSP\*26 and MS 30; FIG. 2: step 104; FIG. 4: connection between CSP\*26 and MS 30; FIG. 5: connection between CT\* 76 and MS 30; and FIG. 6: step 164), the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface (e.g., specification at page 5, lines 12 - 21; FIG. 1: SIM-WIM 32; FIG. 4: SIM-WIM 32; FIG. 5: SIM-WIM 32), and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 44 are directed to:

44. A mobile communications device (e.g., MS 30), the mobile communications device being able to communicate over a first wireless interface with a telecommunications network (e.g., specification at page 4, lines 20-33), and comprising a cryptographic module (e.g., SIM-WIM 32) to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface (e.g., Security Manager 38), wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module (e.g., FIG. 3, step 134), and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface (e.g., FIG. 3, step 138).

Embodiments defined by independent claim 47 are directed to:

47. A module for a computer system, the module comprising:  
an application interface (e.g., CAPI 18) for connection to a computer application (e.g., e-mail application 14; browser 16); and  
an external interface (e.g., FIG. 1: connection between CSP\*26 and MS 30; FIG. 5: connection between CT\* 76 and MS 30) for connection to a mobile communication device (e.g., MS 30) containing a cryptographic module (e.g., SIM-WIM 32);  
wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom (e.g., specification at page 6, lines 17-28).

Claim 48 depends from 47 and further defines that “the module has some cryptographic functionality, and comprises means (e.g., CSP\* 26; specification at page 6, lines 17-28) for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function.” The “means for determining” are defined in terms of means-plus-function as permitted by 35 U.S.C. §112, sixth paragraph.

Exemplary supporting structure/material/acts for these elements are described in the application as just indicated.

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Applicant respectfully requests review of the following grounds of objection/rejection:

1. The objection to the specification as allegedly failing to provide proper antecedent basis for the claimed subject matter. (See 37 CFR 1.75(d)(1) and MPEP §608.01(o).) And, the rejection of claims 1-19, 28-30, and 32-46 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.
2. The rejection of claims 47 and 48 under 35 U.S.C. §102(b) as allegedly being anticipated by Caputo et al. (U.S. Patent 5,778,071) (hereinafter “Caputo”).
3. The rejection of claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Liebenow et al. (U.S. Patent 6,131,136) (hereinafter “Liebenow”).
4. The rejection of claims 5, 8, 9, 41, and 46 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Ericsson, “Bluetooth - A Global Specification for Wireless Connectivity” (hereinafter “Ericsson”).
5. The rejection of claim 49 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Ericsson.
6. The rejection of claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Geiger et al. (US Patent 6,463,534 B1) (hereinafter, “Geiger”).
7. The rejection of claims 43 and 45 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of RSA, “PKCS #11 v2.10: Cryptographic Token Interface Standard” (hereinafter “RSA”).

8. The rejection of claim 50 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of RSA.

## VII. ARGUMENT

All of the objections and rejections set forth in the Final Office Action of May 3, 2006 are traversed in the following arguments:

1. **The specification provides proper antecedent basis for the claimed subject matter as required under 37 CFR 1.75(d)(1), and satisfies the written description requirement under 35 U.S.C. §112, first paragraph**

In the Final Office Action, the Examiner objected to the specification on the grounds that the specification does not provide antecedent basis for a number of limitations added to claims 1, 7, 19, 28, 36, and 44 in Applicant's Amendment filed on January 5, 2006. Additionally, claims 1-19, 28-30, and 32-46 were rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. The Examiner's entire explanation of this rejection was: "See objection to specification." Because the rejection under the first paragraph of Section 112 appeared to be based on the lack of antecedent basis cited above with respect to the objection to the specification, these two issues are discussed herein together.

In order to reduce the number of issues to be resolved on Appeal, Applicant filed an After-Final Amendment on July 25, 2006, in which it was proposed to amend the specification to provide antecedent basis for terminology used to describe elements/steps in the claims, which elements/steps were already supported by the originally-filed application. (See, e.g., Figs.1-3 and the supporting text spanning page 3, line 19 through page 8, line 28 of the originally-filed application.)

It was believed that these amendments would address all of the Office's concerns except for one, namely, the concern that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36." In response to this objection, Applicant's remarks noted that the Examiner had erred in parsing the claim. As amended, claim 36 does *not* define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device." That is, the claimed system comprises two distinct elements (i.e.,

the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification were believed to be necessary to address this aspect of the Office's concern.

Having addressed the Examiner's stated concerns (i.e., lack of antecedent basis in the specification) upon which were based the objection to the specification and the rejection of claims under 35 U.S.C. §112, first paragraph, Applicant was surprised to receive an Advisory Action explaining that the proposed amendments to the specification would not be entered on the grounds that "they raise the issue of new matter," because Applicant would have expected the issue of new matter to be raised with respect to the claims in the Final Office Action. Nonetheless, Applicant will now address the issues of antecedent basis as well as new matter.

Because Applicant's proposed amendments to the specification were not entered, the specification does not include word for word support of the language presently recited in claims 1, 7, 19, 28, 36, and 44. However, it is well known that "the invention claimed does not have to be described in *ipsis verbis* in order to satisfy the description requirement of Sec. 112." In re Wright, 866 F.2d 422, 424 (Fed. Cir. 1989). Instead, it is sufficient if "the meaning of [the claim language in question] is sufficiently described in the specification to inform the public what said language is intended to encompass." *Id.*

It is respectfully asserted that the meaning of the claim language introduced in the amendment of January 5, 2006 was sufficiently described in the specification to satisfy all statutory requirements. In particular, the last paragraph of claim 1 was amended as follows:

using the cryptographic module of the mobile communications device[[,]] as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.

Claim 7 was similarly amended to define "means for connection to a remote computer without involving the wireless communications network."

Claim 19 was amended to define:

the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that

the ~~mobile communications device~~ cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network

Claim 28 was amended to define “using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network.”

Claim 36 was amended to define:

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

And claim 44 was amended to define:

wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface.

In each instance, the Examiner objected that the specification does not support claims that include a mobile communications device performing the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network.

This objection is without merit. For example, the specification at page 3, lines 26-30, expressly states that “[t]he computer has a connection to an external network 12, for example through a modem (not shown).” The connection to the network 12 is illustrated in FIG. 1, and it can clearly be seen that the connection does not involve the mobile station 30.

The text spanning page 3, line 31 through page 4, line 19 clearly sets forth an intention to provide cryptographic functionality to applications running in the computer, which applications are communicating with the network 12 via the computer's own connection to that network.

A solution, described in the specification text spanning page 4, line 20 through page 8, line 28 involves a mobile station 30 providing the desired cryptographic functionality for the computer. As described on page 6, lines 1-16, there is a communication link established between the computer and the mobile station so that the computer can request the desired functionality, and the mobile station can return the desired results.

It is clear from the description that the mobile station does not pass the cryptographic results on to its own wireless network, but rather returns these results to the computer. For example, FIG. 2 is a flowchart showing a method by which the PC 10 can use the cryptographic functionality in the mobile phone 30. As explained on page 8, lines 4-7 of the specification, "In step 112, the result of the operation in the MS 30 is sent to the CSP\*26, and then to the CAPI 18. In step 114, the CAPI 114 [sic: 18], then responds to the application which requested the cryptographic functionality."

Since the application that requested the cryptographic functionality is using the computer's own connection to the network 12 (see e.g., FIG. 1), there is no need for the encrypted data to pass back through the mobile phone 32 to the wireless network. Thus, no such action is described in the specification.

That the mobile communications device performs the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network is further supported by the specification text at page 8, lines 8-28, in conjunction with FIG. 3, which is a flowchart showing the operation carried out in the MS 30. Of relevance here is that the MS 30 carries out the requested cryptographic operation (step 136), and "[t]hen, in step 138, the result of the cryptographic operation is sent back to the PC over the previously established communication link." It will be observed that sending the cryptographic operation result back to the PC is the final step carried out in the MS 30, because there is no need for the MS 30 to involve its own wireless network.

It should be clear from the foregoing remarks that the various instances of claim language defining a mobile communications device performing a cryptographic function for a computer without sending the results of the cryptographic function over the wireless network are well-supported in the specification.



As to the Examiner's additional allegation that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36," Applicant again respectfully asserts that the Examiner has erred in parsing the claim. As amended, claim 36 does not define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device." That is, the claimed system comprises two distinct elements (i.e., the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification are believed to be necessary to address the Office's concern.

Accordingly, the objection to the specification as lacking antecedent basis, and the rejection of claims 1-19, 28-30, and 32-46 under the first paragraph of 35 U.S.C. §112 (regardless of whether the basis for the rejection is lack of antecedent basis or an allegation of new matter) should be reversed.

**2. Claims 47 and 48 are not anticipated under 35 U.S.C. §102(b) by Caputo et al. (U.S. Patent 5,778,071) (hereinafter "Caputo") because they each define subject matter that is neither found nor suggested in Caputo**

Claim 47 defines "A module for a computer system, the module comprising: an application interface ...; and an external interface for connection to a mobile communication device containing a cryptographic module; *wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.*" (Emphasis added.)

Claim 48 depends from 47 and further defines that "the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function."

Neither of claims 47 and 48 is anticipated by Caputo because Caputo fails to disclose or suggest a division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device so that the computer comprises "a cryptographic module; wherein, *when the module receives from the application interface a request for a cryptographic*

*function which the module is unable to provide*, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom,” as defined by claim 47. Caputo is similarly silent with respect to claim 48's recitation of “the module [having] some cryptographic functionality, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function.”

The Office Action of August 5, 2005 had alleged that the Caputo patent, at column 15 lines 13-39, discloses a computer comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto. In response to this allegation, Applicant pointed out (in the Amendment of January 5, 2006) that the cited portion of Caputo merely describes two modes of operation: one in which the device 10 encrypts the data and immediately sent it to the network 20, and another in which the device 10 performs the encryption but then returns the encrypted data to the computer 22 for subsequent transmission to the network 20, possibly as part of another message. Nowhere does this passage describe a computer having its own cryptographic capabilities separate and apart from those provided by the device 10.

The Final Office Action repeats the allegation that the subject matter of claims 47 and 48 is anticipated by the Caputo patent but appears to construe these claims as merely defining the computer sending commands to the cryptographic module. As to features such as “when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom,” as defined by claim 47, and “the module [having] some cryptographic functionality, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function,” as defined by claim 48, the Final Office Action states, on page 22, that “it is noted that the features upon which applicant relies ... are not recited in the rejected claim(s).” However, a reading of these claims shows that this is incorrect.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 47 and 48 under 35 U.S.C. §102(b) be reversed.

3. **Claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 define subject matter that is novel and nonobvious over Caputo in view of Liebenow et al. (U.S. Patent 6,131,136) (hereinafter “Liebenow”)**

Embodiments defined by independent claims 1, 7, 19, 24, 28, 36 and 44 (as well as their related dependent claims 4, 6, 11, 13-15, 18, 26-27, 32-34, 37-39, and 42) are believed to be patentably distinguishable over the prior art of record because they include novel and nonobvious features that enable a single mobile communications device to achieve a unique efficiency in that *a same cryptographic module located in the mobile communications device is used not only to support the device’s own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.* In this respect, it is important to understand that the personal computer is *not* communicating *through* the mobile communications device and the wireless network to get to its own network; its exchanges with the mobile communications device are merely for the purpose of utilizing the cryptographic functions that the mobile communications device can offer.

Specific claimed features lacking in Caputo and Liebenow are discussed in the following sections A through E, followed by an additional discussion of why the Liebenow patent does not make up for the deficiencies of Caputo.

A. **Neither Caputo nor Liebenow et al. (U.S. Patent 6,131,136) (hereinafter “Liebenow”) disclose “establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication”**

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because *a same cryptographic module located in the mobile communications device is used not only to support the device’s own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.* To that end, independent claim 1 defines “establishing a connection with a mobile communications device, wherein said mobile communications device includes a *cryptographic module for use in mobile communication,*” (emphasis added) and each of independent claims 7, 19, 24, 28, 36, and 44 uses the same or

similar language to define a comparable feature. Neither of the Caputo or Liebenow documents discloses or suggests this feature.

In support of its rejection, the Final Office Action asserts that Caputo discloses this claimed feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38.

Applicant respectfully disagrees because the cryptographic circuitry disclosed by Caputo is not “for use in mobile communication over a wireless communications network” as variously required by the claims. Instead, the Caputo device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: “Further, the connector port 14 is a modular receptacle which may be directly connected to a data transfer path, such as a telephone system.”) Thus, there would be absolutely no need for Caputo’s cryptographic circuitry to be for use in mobile communication over a wireless communications network.

Liebenow fails to make up for the deficiencies of Caputo at least because it does not even discuss cryptography. Consequently, any combination of Caputo with Liebenow would still lack this feature.

**B. Neither Caputo nor Liebenow disclose “using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network”**

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. When the mobile communications device is operating on its own behalf, its encrypted communications can be sent over the wireless communications link. However, when the mobile communications device is operating for the benefit of the computer, it merely returns the encrypted result to the computer without involving the wireless communications network. Independent claims 1, 7, 19, 28, 36, and 44 thus variously define “using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.”

The Final Office Action asserts that Caputo discloses this feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38. Applicant respectfully disagrees because, one principle of operation taught by Caputo is that Caputo's computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Consequently, even if the Caputo device 10 were modified to have wireless mobile communications capability (i.e., communicating with a wireless network), the external device 10 of Caputo would still be the computer's only path to the network. Thus, the computer would have to use the hypothetically-modified wireless mobile communications device to access its computer network through the wireless communications network. Such use would be contrary to the requirement that the cryptographic module be used to “encrypt[] said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.” Liebenow fails to make up for the deficiencies of Caputo at least because it, too, is a pass-through device, and does not suggest returning any cryptographic results to the attached computer.

**C. Neither Caputo nor Liebenow disclose a dual-mode cryptographic module that is both “for use in mobile communication over a wireless communications network” and also “us[ed] ... as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network”**

Independent claim 1 defines “a cryptographic module for use in mobile communication over a wireless communications network” and also “using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.” Independent claims 7, 19, 24, 28, 36, and 44 variously define comparable features. Neither Caputo nor Liebenow discloses or suggests this feature, and any combination of these two teachings would similarly lack the claimed limitations.

The device of Caputo appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs cryptographic functions as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism in which the cryptographic module of the mobile communication device is “for use in mobile communication over a wireless communications network” and also for “[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network.” Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography, and therefore cannot suggest a dual-mode cryptographic module as claimed.

**D. Neither Caputo nor Liebenow disclose a system in which “a first part of the required cryptographic functionality [is] provided in the computer, and a second part of the required cryptographic functionality [is] provided in the mobile communications device”**

Independent claim 24 further defines “a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device.”

As explained earlier with respect to the rejection of claims 47 and 48, Caputo fails to disclose or suggest this claimed feature because it is silent with respect to any division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device.

Also as mentioned earlier, the Final Office Action states, on page 22, that “it is noted that the features upon which applicant relies ... are not recited in the rejected claim(s).” However, a reading of claim 24 shows that this is incorrect.

Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography. Consequently, any combination of Caputo with Liebenow would still lack the claimed feature.

**E. Neither Caputo nor Liebenow disclose a system in which “the computer further compris[es] an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto”**

Claim 24 additionally defines “the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.” This feature is related to the feature discussed above in Section D, wherein a first part of the required cryptographic functionality is provided in the computer, and a second part of the required cryptographic functionality is provided in the mobile communications device. The claimed “interface” provides the capability of selecting which of the two cryptographic functionality service providers will be used when needed.

As Caputo is lacking any disclosure of some cryptographic functionality being performed in the computer, and some cryptographic functionality being performed in the mobile communications device, it follows that Caputo does not describe an interface for selecting one of the two. Liebenow, which is silent with respect to cryptographic functionality, fails to make up for the deficiencies of Caputo.

**F. Any combination of Caputo's teachings with the teachings of Liebenow would still lack features variously defined by Applicant's claims**

The Final Office Action acknowledges that Caputo does not disclose, at least, a mobile communication device that is also usable over a wireless communications network, but relies on Liebenow as making up for this deficiency. This reliance is unfounded, at least for the reasons discussed above in Sections A through E.

Moreover, Applicant believes that Liebenow cannot be considered to disclose a mobile communication device, as that term is used in Applicant's specification. Instead, Liebenow discloses a dual mode modem that automatically switches between a wireless and wire-based communication modes using mode selection circuitry that detects when a wire-based communications network, such as a standard land-line telephone network, is coupled to the modem. Such a device fails to satisfy Applicant's variously-worded definitions of "said mobile communications device includ[ing] a cryptographic module for use in mobile communication over a wireless communications network." (See, e.g., independent claims 1, 7, 19, 24, 28, 36, and 44.) Rather, Liebenow's dual mode modem is more of a dumb, slave device that could never be used on its own; it would therefore never require its own cryptographic module *for use in mobile communication over a wireless communications network*, as required by Applicant's claims. Consequently, any combination of Caputo with Liebenow would still lack this claimed feature.

Moreover, even if Caputo's device were modified to include Liebenow's dual mode capability, the combination would still operate in only one mode, namely, for the benefit of the external device (computer), operating only to pass data between the computer and its network. All cryptographic functions would be performed only as required by the node that the *computer* is connected to, *and would pass through the device to the computer network*. By contrast, embodiments such as those defined by independent claim 28 require that *the encrypting device return the encrypted data to the computer* for communication over a computer network without sending the encrypted data over the wireless communication



network. See also independent claim 44, which defines “a mobile communications device ... comprising a security manager module ... *[that] returns the results of the cryptographic function to the computer system ....*” (Emphasis added.) Consequently, any combination of Caputo with Liebenow et al. would still lack any dual mechanism in which the cryptographic module of the mobile communication device is “for use in mobile communication over a wireless communications network” and also for “[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network.”

#### **G. Conclusion**

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 under 35 U.S.C. §103(a) be reversed.

#### **4. Claims 5, 8, 9, 41, and 46 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of Ericsson, “Bluetooth -- A Global Specification for Wireless Connectivity” (hereinafter “Ericsson”)**

Claims 5, 8-9, 41, and 46 variously depend from independent claims 1, 7, 36, and 44 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its disclosing the use of Bluetooth technology, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Ericsson would still lack the various combinations of elements defined by claims 5, 8, 9, 41, and 46.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 5, 8, 9, 41, and 46 under 35 U.S.C. §103(a) be reversed.

#### **5. Claim 49 defines subject matter that is novel and nonobvious over Caputo in view of Ericsson**

Claim 49 depends from independent claim 47 and is therefore patentably distinguishable over any combination of Caputo for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its

disclosing the use of Bluetooth technology, also fails to disclose any of the above-identified features that are lacking in Caputo. Consequently, any combination of Caputo with Ericsson would still lack the combinations of elements defined by claim 49.

For at least the foregoing reasons, it is respectfully requested that the rejection of claim 49 under 35 U.S.C. §103(a) be reversed.

**6. Claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of Geiger et al. (US Patent 6,463,534 B1) (hereinafter, “Geiger”)**

Claims 2-3, 10, 12, 16, 17, 25, 29-30, 35, and 40 variously depend from independent claims 1, 7, 24, 28, and 36 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the Geiger document, which was relied on by the Office merely for its disclosing the use of the Wireless Application Protocol (WAP) (utilizing WTLS and a WIM), also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Geiger would still lack the various combinations of elements defined by claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 under 35 U.S.C. §103(a) be reversed.

**7. Claims 43 and 45 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of RSA, “PKCS #11 v2.10: Cryptographic Token Interface Standard” (hereinafter “RSA”)**

Claims 43 and 45 depend from independent claims 36 and 44, respectively, and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the RSA document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and RSA would still lack the various combinations of elements defined by claims 43 and 45.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 43 and 45 under 35 U.S.C. §103(a) be reversed.

**8. Claim 50 defines subject matter that is novel and nonobvious over Caputo in view of the RSA document**

Claim 50 depends from independent claim 47, and is therefore patentably distinguishable over Caputo for at least the reasons discussed above with respect to claim 47. Furthermore, the RSA document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with RSA would still lack the combination of elements defined by claim 50.

For at least the foregoing reasons, it is respectfully requested that the rejection of claim 50 under 35 U.S.C. § 103(a) be reversed.

**9. Conclusion**

Applicant has traversed all of the objections and rejections stated in the Final Office Action, and accordingly believes that the application is now in condition for allowance. It is therefore respectfully requested that all of the objections and rejections raised in the Final Office Action be reversed, and that a Notice of Allowance be mailed to Applicant.

As required under 37 CFR §41.37(c)(1), a Claims Appendix Is Attached Hereto. There is no need for either an Evidence Appendix or a Related Proceedings Appendix.

Respectfully submitted,  
Potomac Patent Group PLLC

Date: November 24, 2006  
P.O. Box 270  
Fredericksburg, Virginia 22404  
703-718-8884

By: /Kenneth B. Leffler, Reg. No. 36,075/  
Kenneth B. Leffler  
Registration No. 36,075

## **VIII. CLAIMS APPENDIX**

The following claims are now pending in the application:

**Claim 1 (previously presented):** A method of encrypting communications from a computer having an application program interface, the method comprising:

- initiating communications from said computer over a computer network;
- determining that encryption of said communications is required;
- establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network; and
- using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.

**Claim 2 (original):** A method as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

**Claim 3 (original):** A method as claimed in claim 1, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

**Claim 4 (previously presented):** A method as claimed in claim 1, wherein the step of establishing a connection with the mobile communications device comprises establishing a wired connection between the mobile communications device and the computer.

**Claim 5 (previously presented):** A method as claimed in claim 1, wherein the step of establishing a connection with the mobile communications device comprises establishing a wireless connection between the mobile communications device and the computer.

**Claim 6 (original):** A method as claimed in claim 1, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

Claim 7 (previously presented):      A mobile communications device, comprising:  
         means for communicating over a wireless interface with a wireless communications network;  
         means for connection to a remote computer without involving the wireless communications network; and  
         a cryptographic module, the cryptographic module being usable:  
             for encoding wireless communications from the device over said wireless interface;  
             by a cryptographic service provider with an application program interface of the remote computer.

Claim 8 (previously presented):      A mobile communications device as claimed in claim 7, wherein the means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer.

Claim 9 (previously presented):      A mobile communications device as claimed in claim 8, wherein the short-range wireless communications transceiver uses Bluetooth wireless technology.

Claim 10 (original):    A mobile communications device as claimed in claim 7, wherein the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security.

Claim 11 (original):    A mobile communications device as claimed in claim 7, wherein the cryptographic module uses public key cryptography.

Claim 12 (original):    A mobile communications device as claimed in claim 7, comprising means for sending and transmitting data using WAP.

Claim 13 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in hardware in the device.

Claim 14 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in software in the device.

Claim 15 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is provided on an external smart card.

Claim 16 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module comprises a Wireless Identity Module card.

Claim 17 (original): A mobile communications device as claimed in claim 16, wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.

Claim 18 (original): A mobile communications device as claimed in claim 7, comprising an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command.

Claim 19 (previously presented): A tangible module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network, the module sends a second command to a mobile communication device, the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network.

Claims 20-23 (canceled)

Claim 24 (previously presented): A system, comprising:

- a computer; and
- a mobile communications device, including a cryptographic module for performing cryptographic functions in mobile communication over a wireless communications network, the computer having at least one application which requires cryptographic functionality for communication over a computer network,
- a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device,
- the computer and the mobile communications device having means for establishing a secure communications path therebetween; and
- the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

Claim 25 (original): A computer system as claimed in claim 24, wherein the mobile communications device is a WAP-enabled device.

Claim 26 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an internal memory access application.

Claim 27 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an external communication application.

Claim 28 (previously presented): A method of encrypting communications from a computer having an application program interface, wherein the communications are over a computer network, the method comprising:

- sending data to be encrypted from the computer to a mobile communications device, wherein the mobile communications device has a cryptographic module for performing cryptographic functions in communications over a wireless communications network, and

further, wherein the mobile communications device uses the cryptographic module to encrypt the data;

receiving encrypted data at the computer from the mobile communications device;  
and

using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network.

**Claim 29 (original):** A method as claimed in claim 28, wherein the mobile communications device is a WAP-enabled device.

**Claim 30 (original):** A method as claimed in claim 28, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

**Claim 31 (canceled)**

**Claim 32 (original):** A method as claimed in claim 28, comprising using a cryptographic module realized in hardware in the mobile communications device.

**Claim 33 (original):** A method as claimed in claim 28, comprising using a cryptographic module realized in software in the mobile communications device.

**Claim 34 (original):** A method as claimed in claim 28, comprising using a cryptographic module provided on an external smart card which can be read by the mobile communications device.

**Claim 35 (original):** A method as claimed in claim 28, comprising using a cryptographic module provided on a Wireless Identity Module card in said mobile communications device.

**Claim 36 (previously presented):** A system for supporting an application, the system comprising:

a computer including:

a cryptographic application program interface; and



a cryptography service provider; and  
a mobile communication device including a cryptographic module,  
wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface sends a command to the cryptography service provider, and

wherein the cryptography service provider has a communications link to the cryptographic module of the mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface, and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

Claim 37 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in hardware in the mobile communications device.

Claim 38 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in software in the mobile communications device.

Claim 39 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on an external smart card which can be read by the mobile communications device.

Claim 40 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on a Wireless Identity Module card in said mobile communications device.

Claim 41 (original): A system as claimed in claim 36, wherein the cryptography service provider has a Bluetooth wireless communications link to the mobile communications device.

Claim 42 (original): A system as claimed in claim 36, wherein the cryptography service provider has some cryptographic functionality, and, on receipt of a command from the cryptographic application program interface, determines whether it can perform the required

cryptographic functionality, or whether to obtain the required cryptographic functionality from the cryptographic module of the mobile communications device.

Claim 43 (original): A system as claimed in claim 36, wherein the communications link between the cryptography service provider and the cryptographic module of the mobile communications device uses a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 44 (previously presented): A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface.

Claim 45 (original): A mobile communications device as claimed in claim 44, wherein the security manager module responds to a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 46 (original): A mobile communications device as claimed in claim 44, wherein the second interface is a Bluetooth short-range radio interface.

Claim 47 (original): A module for a computer system, the module comprising:  
an application interface for connection to a computer application; and  
an external interface for connection to a mobile communication device containing a cryptographic module;  
wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command

over the external interface to the mobile communications device to request the cryptographic function therefrom.

Claim 48 (previously presented): A module for a computer system as claimed in claim 47, wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function.

Claim 49 (original): A module for a computer system as claimed in claim 47, wherein the external interface is a Bluetooth short-range radio interface.

Claim 50 (original): A module for a computer system as claimed in claim 47, wherein the module sends over the external interface a command from a command set as defined in a standard PKCS#11, where the commands are redefined as AT commands.

**IX. EVIDENCE APPENDIX**

None

**X. RELATED PROCEEDINGS APPENDIX**

None

## **EXHIBIT C**

Under the paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2005</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) <div style="text-align: center; font-weight: bold;">0119-082</div>	
Application Number <b>09/977,192</b>		Filed <b>October 16, 2001</b>	
For <b>Security System</b>			
Art Unit <b>2137</b>		Examiner <b>WILLIAMS, Jeffery L</b>	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application. The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):			
	<u>Fee</u>	<u>Small Entity Fee</u>	
<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$120	\$60	\$ _____
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$450	\$225	\$ _____
<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1020	\$510	\$ _____
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$1590	\$795	\$ _____
<input checked="" type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$2160	\$1080	\$ <b>2160</b>
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.			
<input type="checkbox"/> A check in the amount of the fee is enclosed.			
<input checked="" type="checkbox"/> Payment by credit card. <del>XXXXXXXXXXXXXXXXXXXX</del> <b>On-line payment via RAM</b>			
<input type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.			
<input type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <b>50-2476</b> . I have enclosed a duplicate copy of this sheet.			
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>			
I am the <input type="checkbox"/> applicant/inventor.			
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).			
<input checked="" type="checkbox"/> attorney or agent of record. Registration Number <b>36,075</b>			
<input type="checkbox"/> attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____			
<u>/Kenneth B. Leffler, Reg. No. 36,075/</u> Signature		<u>June 25, 2007</u> Date	
<u>Kenneth B. Leffler</u> Typed or printed name		<u>703-718-8884</u> Telephone Number	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input type="checkbox"/> Total of _____ forms are submitted.			

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## **EXHIBIT D**



# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
[REDACTED]	[REDACTED]	125	[REDACTED]
Event Date	Initials	Notes	
10/26/2006	SMD	Patent Application Filed (on or after 6/8/1995)	
11/14/2006	SMD	Notice of Missing Parts (date of mailing)	
		need dec and formal drawings	
11/27/2006	SMD	Postcard received for application filing?	
1/16/2007	SMD	Last day to respond to Notice of Missing Parts (extension available)	
1/26/2007	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)	
1/26/2007	SMD	Filing receipt received for filing application?	
1/26/2007	SMD	Assignment document(s) filed?	
2/14/2007	SMD	Last day to respond to Notice of Missing Parts (four one-month extensions available)	
3/14/2007	SMD	Last day to respond to Notice of Missing Parts (three one-month extensions available)	
4/16/2007	SMD	Last day to respond to Notice of Missing Parts (two one-month extension available)	
4/26/2007	SMD	Formal Drawings filed?	
5/14/2007	SMD	Last day to respond to Notice of Missing Parts (one one-month extension available)	
4/28/2008	SMD	Publication of patent due	
10/26/2008	SMD	Submit status inquiry	
10/26/2026	SMD	Patent expires, unless eligible for up to 5 years extension due to prosecution delays	

[REDACTED]	[REDACTED]	125	[REDACTED]
Event Date	Initials	Notes	
10/26/2006	SMD	Patent Application Filed (on or after 6/8/1995)	
11/14/2006	SMD	Notice of Missing Parts (date of mailing)	
		need dec and formal drawings	
11/27/2006	SMD	Postcard received for application filing?	
1/16/2007	SMD	Last day to respond to Notice of Missing Parts (extension available)	
1/26/2007	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)	
1/26/2007	SMD	Filing receipt received for filing application?	
1/26/2007	SMD	Assignment document(s) filed?	
2/14/2007	SMD	Last day to respond to Notice of Missing Parts (four one-month extensions available)	
3/14/2007		Last day to respond to Notice of Missing Parts (three one-month extensions	

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
	SMD available)		
4/16/2007	SMD Last day to respond to Notice of Missing Parts (two one-month extension available)		
4/26/2007	SMD Formal Drawings filed?		
5/14/2007	SMD Last day to respond to Notice of Missing Parts (one one-month extension available)		
4/28/2008	SMD Publication of patent due		
10/26/2008	SMD Submit status inquiry		
10/26/2026	SMD Patent expires, unless eligible for up to 5 years extension due to prosecution delays		

887

Event Date	Initials	Notes
8/15/2005	SMD	Patent Application Filed (on or after 6/8/1995)
11/15/2005	SMD	Filing receipt received for filing application?
11/15/2005	SMD	Assignment document(s) filed?
11/15/2005	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)
12/29/2005	SMD	Publication of patent due
2/15/2006	SMD	Formal Drawings filed?
8/15/2006	SMD	Submit status inquiry
9/28/2006	SMD	Office Action (date of mailing)
10/12/2006	SMD	Report Action to Client by E-mail
10/26/2006	SMD	Conduct Interview if Appropriate? Prepare Draft Response, submit within 2 mos. of Response mail date.
12/28/2006	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months) File Response unless otherwise Instructed by
1/26/2007	SMD	Response to Office Action Due (4 Mos. ext avail.)
2/28/2007	SMD	Response to Office Action Due (5 Mos. ext avail.)
3/28/2007	SMD	Response to Office Action due, if extended to 6 month maximum
5/14/2007	SMD	Final Office Action (date of mailing)
5/25/2007	SMD	Report Action to
6/25/2007	SMD	Begin Preparing Recommendation for
7/16/2007	SMD	Response Due to Final Office Action (2 month date)
8/14/2007	SMD	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)
8/14/2007	SMD	Respond to Final Office Action 3 Month (extensions available)
9/14/2007	SMD	Respond to Final Office Action 4 Month (extensions available)
9/14/2007	SMD	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
10/15/2007	SMD	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
10/15/2007	SMD	Respond to Final Office Action 5 Month (extensions available)	
11/14/2007	SMD	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
11/14/2007	SMD	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
8/15/2025	SMD	Patent expires, unless eligible for up to 5 years extension due to prosecution delays	

[REDACTED] [REDACTED] 125 [REDACTED]

Event Date	Initials	Notes
10/26/2006	SMD	Patent Application Filed (on or after 6/8/1995)
11/14/2006	SMD	Notice of Missing Parts (date of mailing)
		need dec and formal drawings
11/27/2006	SMD	Postcard received for application filing?
1/16/2007	SMD	Last day to respond to Notice of Missing Parts (extension available)
1/26/2007	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)
1/26/2007	SMD	Filing receipt received for filing application?
1/26/2007	SMD	Assignment document(s) filed?
2/14/2007	SMD	Last day to respond to Notice of Missing Parts (four one-month extensions available)
3/14/2007	SMD	Last day to respond to Notice of Missing Parts (three one-month extensions available)
4/16/2007	SMD	Last day to respond to Notice of Missing Parts (two one-month extension available)
4/26/2007	SMD	Formal Drawings filed?
5/14/2007	SMD	Last day to respond to Notice of Missing Parts (one one-month extension available)
4/28/2008	SMD	Publication of patent due
10/26/2008	SMD	Submit status inquiry
10/26/2026	SMD	Patent expires, unless eligible for up to 5 years extension due to prosecution delays

[REDACTED] [REDACTED] 298 [REDACTED]

Event Date	Initials	Notes
7/10/2000	SMD	Priority Date First Provisional appn filing date
8/22/2000	SMD	Priority Date Second Provisional appn filing date
9/21/2000	SMD	Patent Application Filed (on or after 6/8/1995)
11/16/2000	SMD	Filing Receipt (date of mailing)

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
12/1/2000	SMD	Information Disclosure Statement (IDS) filing date without fee under 37 C.F.R. 97(b)	
1/16/2001	SMD	Response filed for Missing Parts mailed 11/13/00	
1/16/2001	SMD	Assignment Filing Date (recommended by Patent and Trademark Office to allow entry of application number by attorney)	
3/16/2001	SMD	Last day to respond to Notice of Missing Parts (extension available)	
5/16/2001	SMD	Last day to respond to Notice of Missing Parts (extension available)	
7/5/2001	SMD	Corrected Filing Receipt Received	
1/10/2002	SMD	Publication of patent due	
2/22/2002	SMD	Publication of patent due	
3/21/2002	SMD	Publication of patent due CHECK FILE	
6/24/2004	SMD	Response filing for Nonfinal OA mailed 3/24/04	
5/20/2005	SMD	Office Action (date of mailing)	
8/22/2005	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
10/19/2005	SMD	Final Office Action (date of mailing)	
10/26/2005	SMD	Status Inquiry Office Action	
1/19/2006	SMD	Respond to Final Office Action 3 Month (extensions available)	
1/25/2006	SMD	Final Office Action (date of mailing)	
4/25/2006	SMD	Respond to Final Office Action 3 Month (extensions available)	
4/25/2006	SMD	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
4/25/2006	SMD	Last day for Appellant to file appeal brief (extensions available)	
5/16/2006	SMD	Office Action (date of mailing)	
5/25/2006	SMD	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
5/25/2006	SMD	Respond to Final Office Action 4 Month (extensions available)	
8/16/2006	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
9/18/2006	SMD	Response to Office Action due, (1X)	
10/16/2006	SMD	Response to Office Action due, (2X)	
11/2/2006	SMD	Notice of Allowance from Patent and Trademark Office (date of mailing)	
11/16/2006	SMD	check status	
11/16/2006	SMD	Response to Office Action due, (3X)	
2/2/2007	SMD	Issue Fee Due	
7/10/2020	SMD	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
8/24/2020	SMD	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
9/21/2020	SMD	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
[REDACTED]	[REDACTED]	[REDACTED],370	[REDACTED]

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
Event Date	Initials	Notes	
7/26/2005	SMD	Patent Application Filed - national phase	
8/25/2005	SMD	Postcard received for application filing?	
10/26/2005	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)	
10/26/2005	SMD	Assignment document(s) filed?	
11/26/2005	SMD	Filing receipt received for filing application?	
		Dec filed 10/26/05	
12/21/2006	SMD	Office Action (date of mailing)	
1/26/2007	SMD	Publication of patent due	
3/21/2007	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
4/23/2007	SMD	Response to Office Action due, (1X)	
5/21/2007	SMD	Response to Office Action due,(2X)	
6/21/2007	SMD	Response to Office Action due, (3X)	
7/24/2007	SMD	check status	
7/28/2025	SMD	Patent expires, unless eligible for up to 5 years extension due to prosecution delays	

[REDACTED] [REDACTED] 989 [REDACTED]

Event Date	Initials	Notes
7/29/2005	KBL	Request for Continued Examination filed
10/17/2005	KBL	Office Action (date of mailing)
10/29/2005	KBL	Status Inquiry -- rec'd resp from Exr?
10/31/2005	KVK	Report Action to Client by E-mail
1/17/2006	KBL	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months) File Response unless otherwise Instructed by [REDACTED]
2/17/2006	KBL	Response to Office Action Due (4 Mos. ext avail.)
3/17/2006	KBL	Response to Office Action Due (5 Mos. ext avail.)
4/7/2006	KVK	Final Office Action (date of mailing)
4/17/2006	KBL	Response to Office Action due, if extended to 6 month maximum
4/21/2006	KVK	Report Action to [REDACTED]
5/19/2006	KVK	Begin Preparing Recommendation for [REDACTED] - AUTO CASE
6/7/2006	KVK	Response Due to Final Office Action (2 month date) - AUTO CASE
7/7/2006	KVK	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)
7/7/2006	KVK	Respond to Final Office Action 3 Month (extensions available)
7/7/2006	KVK	Request for Continued Examination filed

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
8/7/2006	KVK	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
8/7/2006	KVK	Respond to Final Office Action 4 Month (extensions available)	
9/7/2006	KVK	Rec'd Next OA?	
9/7/2006	KVK	Respond to Final Office Action 5 Month (extensions available)	
9/7/2006	KVK	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
9/28/2006	KVK	Office Action (date of mailing)	
10/10/2006	KVK	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
10/10/2006	KVK	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
10/12/2006	KVK	Report Action to Client by E-mail	
10/26/2006	KVK	Conduct Interview if Appropriate? Prepare Draft Response, submit within 2 mos. of Response mail date.	
12/28/2006	KVK	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months) File Response unless otherwise Instructed by [REDACTED]	
1/26/2007	KVK	Response to Office Action Due (4 Mos. ext avail.)	
2/28/2007	KVK	Response to Office Action Due (5 Mos. ext avail.)	
3/28/2007	KVK	Response to Office Action due, if extended to 6 month maximum	
5/1/2007	KVK	check status	
5/4/2007	KVK	Final Office Action (date of mailing)	
5/18/2007	KVK	Report Action to [REDACTED]	
6/18/2007	KVK	Begin Preparing Recommendation for [REDACTED]	
7/5/2007	KVK	Response Due to Final Office Action (2 month date)	
8/6/2007	KVK	Respond to Final Office Action 3 Month (extensions available)	
8/6/2007	KVK	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
9/4/2007	KVK	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
9/4/2007	KVK	Respond to Final Office Action 4 Month (extensions available)	
10/4/2007	KVK	Respond to Final Office Action 5 Month (extensions available)	
10/4/2007	KVK	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
11/5/2007	KVK	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
11/5/2007	KVK	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
[REDACTED]		[REDACTED] 248	[REDACTED]

Event Date	Initials	Notes
10/26/2006	KBL	Office Action (date of mailing)
1/26/2007	KBL	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
2/26/2007	KBL	Response to Office Action due,(1X)	
3/26/2007	KBL	Response to Office Action due, (2X)	
4/26/2007	KBL	Response to Office Action due,(3X)	
[REDACTED]	[REDACTED]	[REDACTED],022	[REDACTED]

Event Date	Initials	Notes
9/15/2005	KBL	Last day to file Information Disclosure Statement (IDS) with fee under 37 C.F.R. 97(c)
9/16/2005	KBL	Final Office Action (date of mailing)
11/16/2005	KBL	Response Due to Final Office Action (2 month date)
12/16/2005	KBL	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)
12/16/2005	KBL	Respond to Final Office Action 3 Month (extensions available)
12/16/2005	KBL	Last day for Appellant to file appeal brief (extensions available)
1/17/2006	KBL	Respond to Final Office Action 4 Month (extensions available)
1/17/2006	KBL	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)
2/15/2006	KBL	Request for Continued Examination filed
2/16/2006	KBL	Respond to Final Office Action 5 Month (extensions available)
2/16/2006	KBL	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)
3/15/2006	KBL	Postcard check: Request for Continued Examination
3/16/2006	KBL	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)
3/16/2006	KBL	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)
4/27/2006	KBL	Office Action (date of mailing)
7/27/2006	KBL	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)
8/28/2006	KBL	Response to Office Action due (1X)
9/26/2006	KBL	Final Office Action (date of mailing)
9/27/2006	KBL	Response to Office Action due (2X)
10/27/2006	KBL	Response to Office Action due, (3X)
10/27/2006	KBL	check status - rec'd resp from Exr?
11/27/2006	KBL	Response Due to Final Office Action (2 month date)
12/26/2006	KBL	Resp to Final OA/Notice of Appeal Due - Extendable
1/26/2007	KBL	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)
1/26/2007	KBL	Respond to Final Office Action 4 Month (extensions available)
2/26/2007	KBL	Respond to Final Office Action 5 Month (extensions available)
2/26/2007	KBL	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)
3/18/2007	KBL	Request for Continued Examination filed

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
3/26/2007	KBL	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
3/26/2007	KBL	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
4/18/2007	KBL	Postcard check: Request for Continued Examination	
5/18/2007	KBL	Rec'd Next OA?	
6/15/2007	KBL	Office Action (date of mailing)	
9/17/2007	KBL	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
10/15/2007	KBL	Response to Office Action due (1X)	
11/15/2007	KBL	Response to Office Action due (2X)	
12/17/2007	KBL	Response to Office Action due, if extended to 6 month maximum	

[REDACTED]		[REDACTED] 022	[REDACTED]
Event Date	Initials	Notes	
9/15/2005	KBL	Last day to file Information Disclosure Statement (IDS) with fee under 37 C.F.R. 97(c)	
9/16/2005	KBL	Final Office Action (date of mailing)	
11/16/2005	KBL	Response Due to Final Office Action (2 month date)	
12/16/2005	KBL	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
12/16/2005	KBL	Respond to Final Office Action 3 Month (extensions available)	
12/16/2005	KBL	Last day for Appellant to file appeal brief (extensions available)	
1/17/2006	KBL	Respond to Final Office Action 4 Month (extensions available)	
1/17/2006	KBL	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
2/15/2006	KBL	Request for Continued Examination filed	
2/16/2006	KBL	Respond to Final Office Action 5 Month (extensions available)	
2/16/2006	KBL	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
3/15/2006	KBL	Postcard check: Request for Continued Examination	
3/16/2006	KBL	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
3/16/2006	KBL	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
4/27/2006	KBL	Office Action (date of mailing)	
7/27/2006	KBL	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
8/28/2006	KBL	Response to Office Action due (1X)	
9/26/2006	KBL	Final Office Action (date of mailing)	
9/27/2006	KBL	Response to Office Action due (2X)	
10/27/2006	KBL	Response to Office Action due, (3X)	



**Event Reminders.Date 01/26/07**

[REDACTED] [REDACTED] 247 [REDACTED]

7/13/2007 3:27 PM

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
6/26/2006	MGS	Final Office Action - rec'd 2 OAs from 2 different Examiners	
8/28/2006	MGS	Response Due to Final Office Action (2 month date)	
9/26/2006	MGS	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
9/26/2006	MGS	Respond to Final Office Action 3 Month (extensions available)	
10/26/2006	MGS	Respond to Final Office Action 4 Month (extensions available)	
10/26/2006	MGS	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
11/27/2006	MGS	Respond to Final Office Action 5 Month (extensions available)	
11/27/2006	MGS	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
12/26/2006	MGS	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
12/26/2006	MGS	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
1/12/2007	MGS	Final Office Action (date of mailing)	
1/26/2007	MGS	Report Action to [REDACTED]	
2/12/2007	MGS	Response to final Office Action due for nonstatutory or shortened statutory time period (extension available for up to 2 additional months)	
2/26/2007	MGS	Begin Preparing Recommendation for [REDACTED]	
3/12/2007	MGS	Response Due to Final Office Action (2 month date)	
4/12/2007	MGS	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
4/12/2007	MGS	Respond to Final Office Action 3 Month (extensions available)	
5/14/2007	MGS	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
5/14/2007	MGS	Respond to Final Office Action 4 Month (extensions available)	
5/17/2007	MGS	Advisory Action Mailed	
6/12/2007	MGS	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
		AA mailed 5/17/07	
6/12/2007	MGS	Respond to Final Office Action 5 Month (extensions available)	
		AA mailed 5/17/07	
7/12/2007	MGS	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
7/12/2007	MGS	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
3/2/2021	MGS	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
11/14/2022	MGS	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
[REDACTED]	[REDACTED]	[REDACTED] 370	[REDACTED]

Event Date	Initials	Notes
10/15/2002	SMD	Patent Application Filed (on or after 6/8/1995)
11/21/2002	SMD	Notice of Missing Parts (date of mailing)

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
1/9/2003	SMD	IDS filed under 37 C.F.R. 1.97(b)	
1/15/2003	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b) - IDS Filed	
1/21/2003	SMD	Last day to respond to Notice of Missing Parts (extension available)	
1/22/2003	SMD	Filing Receipt (date of mailing)	
5/13/2003	SMD	Notice of Recordation of Assignment (Recordation Date)	
4/15/2004	SMD	Publication of patent due	
9/8/2004	SMD	Office Action: Restriction Requirement (date of mailing)	
10/8/2004	SMD	First date that response to Restriction Requirement may be due (extensions available)	
11/17/2004	SMD	Office Action (date of mailing)	
2/17/2005	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
4/17/2005	SMD	SC - OA	
5/17/2005	SMD	Response to Office Action due, if extended to 6 month maximum	
5/20/2005	SMD	Final Office Action (date of mailing)	
8/18/2005	SMD	Notice of Appeal filed	
8/22/2005	SMD	Respond to Final Office Action 3 Month (extensions available)	
8/22/2005	SMD	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
12/13/2005	SMD	Office Action (date of mailing)	
3/13/2006	SMD	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)	
4/13/2006	SMD	Response to Office Action due, unless otherwise notified (1X)	
6/26/2006	SMD	Final Office Action (date of mailing)	
8/28/2006	SMD	Response Due to Final Office Action (2 month date)	
9/26/2006	SMD	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
9/26/2006	SMD	Respond to Final Office Action 3 Month (extensions available)	
10/26/2006	SMD	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
10/26/2006	SMD	Respond to Final Office Action 4 Month (extensions available)	
11/2/2006	SMD	Notice of Allowance from Patent and Trademark Office (date of mailing)	
11/27/2006	SMD	Respond to Final Office Action 5 Month (extensions available)	
11/27/2006	SMD	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
12/26/2006	SMD	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
12/26/2006	SMD	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
2/2/2007	SMD	Issue Fee Due	
10/17/2022	SMD	Patent expires (eligible for up to 5 years extension due to prosecution delays)	

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
[REDACTED]	[REDACTED]	[REDACTED],125	[REDACTED]

Event Date	Initials	Notes
10/26/2006	SMD	Patent Application Filed (on or after 6/8/1995)
11/14/2006	SMD	Notice of Missing Parts (date of mailing)
		need dec and formal drawings
11/27/2006	SMD	Postcard received for application filing?
1/16/2007	SMD	Last day to respond to Notice of Missing Parts (extension available)
1/26/2007	SMD	Information Disclosure Statement (IDS) Due without fee under 37 C.F.R. 97(b)
1/26/2007	SMD	Filing receipt received for filing application?
1/26/2007	SMD	Assignment document(s) filed?
2/14/2007	SMD	Last day to respond to Notice of Missing Parts (four one-month extensions available)
3/14/2007	SMD	Last day to respond to Notice of Missing Parts (three one-month extensions available)
4/16/2007	SMD	Last day to respond to Notice of Missing Parts (two one-month extension available)
4/26/2007	SMD	Formal Drawings filed?
5/14/2007	SMD	Last day to respond to Notice of Missing Parts (one one-month extension available)
4/28/2008	SMD	Publication of patent due
10/26/2008	SMD	Submit status inquiry
10/26/2026	SMD	Patent expires, unless eligible for up to 5 years extension due to prosecution delays

[REDACTED]	[REDACTED]	[REDACTED],615	[REDACTED]
------------	------------	----------------	------------

Event Date	Initials	Notes
4/26/2006	KVK	Office Action (date of mailing)
7/26/2006	KVK	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)
8/28/2006	KVK	Response to Office Action due, (1X)
9/26/2006	KVK	Response to Office Action due, (2X)
10/26/2006	KVK	Response to Office Action due, (3X)
1/26/2007	KVK	check status

[REDACTED]	[REDACTED]	[REDACTED],615	[REDACTED]
------------	------------	----------------	------------

Event Date	Initials	Notes
4/26/2006	KVK	Office Action (date of mailing)
7/26/2006	KVK	Response to Office Action due, unless otherwise notified (extensions available for up to 3 additional months)

**Event Reminders.Date 01/26/07**

Page: 13

# Matters Copy of Listing with Events

Event Reminders.Date 01/26/07

Client	Matter Description	Application No.	Matter ID
8/28/2006	MGS	Response Due to Final Office Action (2 month date)	
9/26/2006	MGS	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
9/26/2006	MGS	Respond to Final Office Action 3 Month (extensions available)	
10/26/2006	MGS	Respond to Final Office Action 4 Month (extensions available)	
10/26/2006	MGS	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
11/27/2006	MGS	Respond to Final Office Action 5 Month (extensions available)	
11/27/2006	MGS	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
12/26/2006	MGS	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
12/26/2006	MGS	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
1/12/2007	MGS	Final Office Action (date of mailing)	
1/26/2007	MGS	Report Action to [REDACTED]	
2/12/2007	MGS	Response to final Office Action due for nonstatutory or shortened statutory time period (extension available for up to 2 additional months)	
2/26/2007	MGS	Begin Preparing Recommendation for [REDACTED]	
3/12/2007	MGS	Response Due to Final Office Action (2 month date)	
4/12/2007	MGS	Notice of Appeal Due 3 Month unless otherwise ordered (extensions available)	
4/12/2007	MGS	Respond to Final Office Action 3 Month (extensions available)	
5/14/2007	MGS	Notice of Appeal Due 4 Month unless otherwise ordered (extensions available)	
5/14/2007	MGS	Respond to Final Office Action 4 Month (extensions available)	
5/17/2007	MGS	Advisory Action Mailed	
6/12/2007	MGS	Notice of Appeal Due 5 Month unless otherwise ordered (extensions available)	
		AA mailed 5/17/07	
6/12/2007	MGS	Respond to Final Office Action 5 Month (extensions available)	
		AA mailed 5/17/07	
7/12/2007	MGS	Respond to Final Office Action 6 Month (Avoid application becoming abandoned)	
7/12/2007	MGS	Notice of Appeal Due 6 Month, unless otherwise ordered by Examiner's Answer (extensions available)	
3/2/2021	MGS	Patent expires (eligible for up to 5 years extension due to prosecution delays)	
11/14/2022	MGS	Patent expires (eligible for up to 5 years extension due to prosecution delays)	

## **EXHIBIT E**

Date Rec'd	USSN	Docket No.	Type	Initials
12/11/06	[REDACTED] 73	[REDACTED]	Not of Pub	Rep
	[REDACTED] 911	[REDACTED]	OFF	
	[REDACTED] 207	[REDACTED]	OFF - NTFMP	
	[REDACTED] 917	[REDACTED]	issue notig.	
	[REDACTED] 526	[REDACTED]	Not of Pub	
	[REDACTED] 950	[REDACTED]	OFF - NTFMP	Rep
12/14/06	[REDACTED] 080	[REDACTED]	OFF	Rep
	[REDACTED] 128	[REDACTED]	CORR OFF	
	[REDACTED] 562	[REDACTED]	OA	
	[REDACTED] 025	[REDACTED]	orig ltrs pat [REDACTED]	
	[REDACTED] 344	[REDACTED]	orig ltrs pat [REDACTED]	
	[REDACTED] 134	[REDACTED]	final OA	
	[REDACTED] 143	[REDACTED]	Final OA	
	[REDACTED] 497	[REDACTED]	OA	
	[REDACTED] 486	[REDACTED]	decision on appeal	Rep
12/18/06	[REDACTED] 410	[REDACTED]	NOA	Rep
	[REDACTED] 719	[REDACTED]	issue notice	
	[REDACTED] 854	[REDACTED]	notice to enter into sep	
	[REDACTED] 890	[REDACTED]	NOA	
	[REDACTED] 377	[REDACTED]	Trans of IPER	Rep
	[REDACTED] 784	[REDACTED]	OFF - NTFMP	Rep
12/20/06	[REDACTED] 828	[REDACTED]	OA	Rep
	[REDACTED] 288	[REDACTED]	final OA	
	[REDACTED] 651	[REDACTED]	issue notig	
	[REDACTED] 207	[REDACTED]	updated OFF	
	[REDACTED] 491	[REDACTED]	notice of Pub	Rep
12/21/06	[REDACTED] 511	[REDACTED]	NOA	Rep
	[REDACTED] 717	[REDACTED]	orig ltrs pat [REDACTED]	
	[REDACTED] 044	[REDACTED]	Final OA	
	[REDACTED] 310	[REDACTED]	OA	
	[REDACTED] 895	[REDACTED]	Trans of IPER	
	[REDACTED] 898	[REDACTED]	orig ltrs pat [REDACTED]	
	[REDACTED] 050	[REDACTED]	OFF - NTFMP	Rep
12/22/06	[REDACTED] 634	[REDACTED]	OA	Rep
	[REDACTED] 764	[REDACTED]	notice of Pub	
	[REDACTED] 913	[REDACTED]	" "	
	[REDACTED] 072	[REDACTED]	2nd notice re: time limit	
	[REDACTED] 219	[REDACTED]	elec of species	Rep
1/21/07	[REDACTED] 730	[REDACTED]	trans of WO + ISR	Rep
	[REDACTED] 009	[REDACTED]	OA	
	[REDACTED] 173	[REDACTED]	NOA	
	[REDACTED] 370	[REDACTED]	OA	
	[REDACTED] 063	[REDACTED]	cert of corr	
	[REDACTED] 257	[REDACTED]	" "	
	[REDACTED] 613	[REDACTED]	" "	
	[REDACTED] 079	[REDACTED]	OA	Rep



Date Rec'd	USSN	Docket No.	Type	Initials
1/2/07	██████████ 317	██████████	orig ltrs pat	step
	██████████ 731	██████████	1st notice re: time limit	
	██████████ 792	██████████	notice of receipt of record copy	
	██████████ 780	██████████	1st notice of re: time limit	
	██████████ 128	██████████	OFI + NAA	
	██████████ 050	██████████	updated OFI	
	██████████ 269	██████████	"	
	██████████ 750	██████████	issue notif	
	██████████ 332	██████████	OFI + NTFMP	
	██████████ 652	██████████	not of pub	
	██████████ 325	██████████	OFI + NTFMP	
	██████████ 403	██████████	NOMR	
	██████████ 950	██████████	updated OFI	
	██████████ 400	██████████	notice of aband	
1/4/07	██████████ 360	██████████	1st notice re: time limit	step
	██████████ 404	██████████	NAA	
	██████████ 309	██████████	"	
1/5/07	██████████ 719	██████████	orig ltrs pat	step
	██████████ 772	██████████	OFI	
1/8/07	██████████ 130	██████████	OFI - NTFMP	step
	██████████ 154	██████████	EP notice of app #	
	██████████ 256	██████████	notice of receipt of record copy	
	██████████ 859	██████████	final OA	
	██████████ 526	██████████	JA	
	██████████ 151	██████████	orig us patent	
	██████████ 459	██████████	cert of corr	
	██████████ 499	██████████	cert of corr	
1/10/07	██████████ 098	██████████	OFI	step
	██████████ 346	██████████	OFI - NTFMP	
	██████████ 128	██████████	OFI - NTFMP	
	██████████ 750	██████████	OFI	
	██████████ 933	██████████	cert of corr	
1/12/07	██████████ 377	██████████	notice of accept	step
	██████████ 090	██████████	OA	
	██████████ 403	██████████	OFI - NAA	
	██████████ 663	██████████	cert of corr	
1/15/07	██████████ 267	██████████	OA	step
	██████████ 247	██████████	final OA	
	██████████ 803	██████████	cert of corr	
	██████████ 379	██████████	notice of accept of POA	
	██████████ 486	██████████	notice of abandon	
	██████████ 134	██████████	notice of recordation	
	██████████ 135	██████████	"	
	██████████ 403	██████████	OFI - NAA	
	██████████ 137	██████████	"	
1/18/07	██████████ 852	██████████	issue notification	step

Date Rec'd	USSN	Docket No.	Type	Initials
1/18/07	866		NonPR	dep
1/19/07	955		Exr's answer	dep
	950		Orig ltr's pat	
	050		Respo to Reg for Corr 5/12/06	
	867		OFR	
	153		Notice of in complete PR/app	dep
	867		OFR	dep
1/22/07	188		Notice of aband	dep
1/23/07	488		Out of corr	dep
	389		AA	
	853		OFR	
	677		OFR	dep
	035		Final OA	dep
1/26/07	243		OFR	
	778		OFR	
	779		OFR	
	906		OFR-NTRMP	
	494		Notice of fees, app # & filing date	
	323		Trans of IP	
	376		Trans of ISL + WO	
	135		OFR	
	129		OFR	
	997		OFR	
	424		Notice of aband	
	621		OFR	
	907		"	
	622		"	
	298		"	
	907		OA	dep
1/27/07	134		OFR	dep
	067		OFR	dep
2/8/07	827		OA	dep
	360		OA	
	852		Orig ltr's pat	
	677		OA	
	132		Notice of pub	
	854		NOA	
	842		OFR - NAA	
	011		Notice of accept of PUA	
	256		Notice relating to priority claim	
	494		notice re second copy	
	292		OFR	
	092		OFR	
	028		"	
	162		OFR/NTRMP	
	303		notice of fees / app #	dep